ABSTRACT OF THE DISCLOSURE

A method and architecture for secure transmission of data within optical-switched networks. In one embodiment, the optical switched network comprises a photonic burst-switched (PBS) network. Under various schemes, security keys including encryption and decryption keys are generated by edge nodes and the decryption keys are distributed to other edge nodes in a PBS network. In one embodiment, the security keys are dynamically generated by a trusted platform module (TPM). A source edge node uses its encryption key to encrypt selected data bursts to be sent to a destination edge node via a virtual lightpath coupling the source and destination edge nodes. Security data are embedded in a control burst header indicates to the destination node whether corresponding data bursts sent via the virtual lightpath are encrypted. The security data also includes the decryption key and may also identify an encryption/decryption algorithm to be used. In some embodiments, public key infrastructure facilities are used in conjunction with employment of private and public keys and digital certificates.